Amendments to the Claims:

Please amend the claims as indicated.

1. (Currently amended) A method for controlling an external storage device connected to a computer; the method comprising the steps of:

detecting that the external storage device is connected to the computer and checking whether or not an encrypted data file is stored in the external storage device;

if an encrypted data file is stored in the external storage device, reading the encrypted data file, decrypting the encrypted data file using a passphrase preset and held by predetermined storage means, and storing the decrypted data file in the external storage device;

accepting an operation by a user and issuing an ejection request to the external storage device connected to the computer in accordance with specifications specifying that software control should be performed, including processing to stop access to the device, when ejection is performed; and

reading and encrypting with a user passphrase the~~a predetermined~~ data file stored in the external storage device and storing the encrypted data file in the external storage device, if the ejection request has been issued, wherein the user inputs the user passphrase and the data file is encrypted with an algorithm selected from RC2, RC4, RC5, RC6, 3DES and AES encryption algorithms.

2. (Original) The method according to claim 1, wherein the method is affixed in a machine readable program.

3. (Canceled)

4. (Currently amended) The method according to claim [[3]]1, wherein the method is affixed in a machine readable program.

5. (Currently amended) A program for controlling a computer to provide encryption processing for a data file stored in an external storage device connected to the computer; the program stored in a memory, executed by a CPU and causing the computer to function as:

decryption means for detecting that the external storage device is connected to the computer, decrypting an encrypted data file stored in the external storage device, and storing the decrypted data file in the external storage device;

acceptance means for accepting an ejection request to the external storage device connected to the computer in accordance with specifications specifying that software control should be performed, including processing to stop access to the device, when ejection is performed; and

encryption means for encrypting with a user passphrase the~~a predetermined~~ data file stored in the external storage device if the ejection request has been accepted by the acceptance means, wherein a user inputs the user passphrase and the data file is encrypted with an algorithm selected from RC2, RC4, RC5, RC6, 3DES and AES encryption algorithms.

6. (Canceled)

7. (Currently amended) The program according to Claim 5, further causing the computer to function as passphrase managing means for managing [[a]]each passphrase used for encryption by the encryption means and decryption by the decryption means.

8. (Currently amended) The programmethod according to claim 5, wherein the programmethod is configured asaffixed in a machine readable program.

9. (Canceled)

10. (Currently amended) A program for controlling a computer to provide encryption processing for a data file stored in an external storage device connected to the computer; the program stored in a memory, executed by a CPU and causing the computer to execute the processes of:

detecting that the external storage device is connected to the computer and checking whether or not an encrypted data file is stored in the external storage device; and

if an encrypted data file is stored in the external storage device, reading the encrypted data file, decrypting the encrypted data file using a passphrase preset and held by predetermined storage means, and storing the decrypted data file in the external storage device[[.]];

accepting an operation by a user and issuing an ejection request to the external storage device connected to the computer in accordance with specifications specifying that software

control should be performed, including processing to stop access to the device, when ejection is performed; and

reading and encrypting with a user passphrase the data file stored in the external storage device and storing the encrypted data file in the external storage device, if the ejection request has been issued, wherein the user inputs the user passphrase and the data file is encrypted with an algorithm selected from RC2, RC4, RC5, RC6, 3DES and AES encryption algorithms.

11. (Original) The program according to claim 10, wherein said program is resident on a computer.

12. (Currently amended) The program according to claim 10, wherein said program is an application re[[a]]sident on a server.